Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 13/22

(Certification No.)

Prodotto: FIN.X RTOS SE V5

(Product)

Sviluppato da: MBDA Italia S.p.A.

(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

Conforme a: Protection Profile for General Purpose Operating Systems v4.2.1

(Conformant to)

(ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1)

Il Direttore
(Dott.ssa Eva Spina)

Firmato digitalmente
da Eva Spina
Data: 2022.06.21
13:08:17 +02'00'

Roma, 21 giugno 2022

Common Criteria

SOGIS IT SECURITY CERTIFIED

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

FIN.X RTOS SE V5

OCSI/CERT/LEO/08/2021/RC

Versione 1.0

21 giugno 2022

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	21/06/2022

2 Indice

3 Elenco degli acronimi

ACL	Access Control List
ASCII	American Standard Code for Information Interchange
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CD-ROM	Compact Disk - Read-Only Memory
CEM	Common Evaluation Methodology
CPU	Central Processing Unit
DAC	Discretionary Access Control
DPCM	Decreto del Presidente del Consiglio dei Ministri
DVD-ROM	Digital Versatile Disc - Read-Only Memory
EAL	Evaluation Assurance Level
GB	Gigabyte
HW	Hardware
IPC	Inter-Process Communication
IT	Information Technology
FP	Functional Package
LGP	Linea Guida Provvisoria
LUKS	Linux Unified Key Setup
LVS	Laboratorio per la Valutazione della Sicurezza
NIAP	National Information Assurance Partnership
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
PAM	Pluggable Authentication Module
PC	Personal Computer

PP	Protection Profile
RAM	Random Access Memory
RFV	Rapporto Finale di Valutazione
SAR	Security Assurance Requirement
SATA	Serial Advanced Technology Attachment
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSH	Secure Shell
TDS	Traguardo di Sicurezza
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
USB	Universal Serial Bus

4 Riferimenti

4.1 Criteri e normative

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CC-STL] CCDB-2006-04-004, “ST sanitising for publication”, April 2006

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

4.2 Documenti tecnici

[FPSSH] Functional Package for Secure Shell (SSH), Version 1.0, NIAP, 13 May 2021

[FPTLS] Functional Package for Transport Layer Security (TLS), Version 1.1, NIAP, 1st March 2019

[PPGPOS] Protection Profile for General Purpose Operating Systems, Version 4.2.1, NIAP, 22 April 2019

[RC] “Rapporto di Certificazione FIN.X RTOS SE V4.0”, OCSI/CERT/RES/06/2014/RC, versione 1.0, 25 luglio 2017

[RFV] Rapporto Finale di Valutazione “FIN.X RTOS SE V5”, CR4AB62RFV01, Rev. 0, Leonardo S.p.A., 3 giugno 2022

[SUM] “Software User Manual for the CSCI FIN.X RTOS SE V5”, ID 16210066680, Rev. 02, MBDA Italia S.p.A., 11 maggio 2022

[SVD] “Software Version Document for the FIN.X RTOS SE V5”, ID 16210067034, Rev. 02, MBDA Italia S.p.A., 11 maggio 2022

[TDS] “FIN.X RTOS SE V5.0 Security Target”, ID 16210063305, Rev. 02, MBDA Italia S.p.A., 11 maggio 2022

[TDS-LITE] “FIN.X RTOS SE V5.0 Security Target (Lite)”, ID 16210068210, Rev. 02, MBDA Italia S.p.A., 11 maggio 2022

5 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA)

L'accordo di mutuo riconoscimento in ambito europeo (SOGIS-MRA, versione 3, [SOGIS]) è entrato in vigore nel mese di aprile 2010 e prevede il riconoscimento reciproco dei certificati rilasciati in base ai Common Criteria (CC) per livelli di valutazione fino a EAL4 incluso per tutti i prodotti IT. Per i soli prodotti relativi a specifici domini tecnici è previsto il riconoscimento anche per livelli di valutazione superiori a EAL4.

L'elenco aggiornato delle nazioni firmatarie e dei domini tecnici per i quali si applica il riconoscimento più elevato e altri dettagli sono disponibili su https://www.sogis.eu/.

Il logo SOGIS-MRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito SOGIS-MRA per tutti i componenti di garanzia dichiarati selezionati dai CC Parte 3 [CC3].

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su https://www.commoncriteriaportal.org/.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA per tutti i componenti di garanzia dichiarati selezionati dai CC Parte 3 [CC3].

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "FIN.X RTOS SE V5", sviluppato dalla società MBDA Italia S.p.A.

L'ODV è un sistema operativo di tipo real-time basato su Linux, derivato dalla distribuzione Gentoo Linux, le cui principali caratteristiche sono l'elevata flessibilità, scalabilità, configurabilità e possibilità di personalizzazione, che lo rendono particolarmente adatto da ottimizzare per i sistemi *embedded*.

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Il presente Rapporto di Certificazione è stato emesso a conclusione della ri-certificazione di una precedente versione dello stesso ODV (FIN.X RTOS SE V4.0), già certificato dall'OCSI (Certificato n. 2/17 del 25 luglio 2017 [RC]) per il livello di garanzia EAL4+.

Su richiesta del Fornitore MBDA Italia S.p.A., la nuova versione dell'ODV è stata certificata per soddisfare i requisiti del Protection Profile for General Purpose Operating Systems v4.2.1 [PPGPOS] del NIAP.

In considerazione della conformità *exact* richiesta da tale PP, che presenta un livello di garanzia diverso rispetto alla precedente valutazione e che ha portato alla riscrittura completa del Traguardo di Sicurezza [TDS], l'LVS Leonardo ha proceduto ad una rivalutazione completa del nuovo ODV "FIN.X RTOS SE V5".

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti e/o utilizzatori. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per i componenti di garanzia inclusi nel PP [PPGPOS], in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

È stato fornito per la pubblicazione un Traguardo di Sicurezza "Lite" [TDS-LITE]. Si tratta di una versione emendata del Traguardo di Sicurezza [TDS] utilizzato per la valutazione,

da cui sono state rimosse informazioni tecniche riservate e proprietarie. La versione “Lite” del TDS è stata prodotta in conformità al documento di supporto del CCRA [CC-STL]

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "FIN.X RTOS SE V5" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti e/o utilizzatori per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

Il presente Rapporto di Certificazione deve essere consultato congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	FIN.X RTOS SE V5
Traguardo di Sicurezza	"FIN.X RTOS SE V5.0 Security Target", Rev. 02 [TDS]
Livello di garanzia	Conforme a PP con i seguenti componenti di garanzia: ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1 e AVA_VAN.1
Fornitore	MBDA Italia S.p.A.
Committente	MBDA Italia S.p.A.
LVS	LVS Leonardo
Versione dei CC	3.1 Rev. 5
Conformità a PP	Protection Profile for General Purpose Operating Systems v4.2.1 [PPGPOS] con i seguenti FP: • Functional Package for Secure Shell (SSH) v1.0 [FPSSH] • Functional Package for Transport Layer Security (TLS) v1.1 [FPTLS]
Data di inizio della valutazione	22 luglio 2021
Data di fine della valutazione	3 giugno 2022

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

7.3 Prodotto valutato

In questo paragrafo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV è il prodotto "FIN.X RTOS SE V5", un sistema operativo multiutente e multitasking di tipo real-time basato su Linux, derivato dalla distribuzione Gentoo Linux, le cui principali caratteristiche sono l'elevata flessibilità, scalabilità, configurabilità e possibilità di personalizzazione, che lo rendono particolarmente adatto da ottimizzare per i sistemi *embedded*.

Per una descrizione dettagliata dell'ODV, si faccia riferimento al par. 1.5 e al par. 1.6 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito.

7.3.1 Architettura dell'ODV

L'ODV fornisce una piattaforma utilizzabile per una gran numero di applicazioni e fornisce un ambiente di esecuzione sicuro in cui l'interazione con le entità esterne è consentita solo attraverso canali attendibili.

L'ODV può essere configurato per eseguire un *kernel* integrato con la patch PREEMPT_RT o un *kernel* senza tale patch. Nella configurazione con la suddetta patch l'ODV fornisce un supporto adeguato ad applicazioni con requisiti real-time.

La valutazione dell'ODV copre una rete potenzialmente distribuita di sistemi che adottano le versioni e le configurazioni valutate dell'ODV.

L'ODV non richiede alcuna piattaforma hardware specifica per funzionare. Esso è in grado di funzionare su tutte le piattaforme architetturali Intel x86_64 in possesso dei seguenti requisiti minimi:

- UEFI Secure Boot
- Microprocessore: Intel Pentium i686 o Intel Xeon
- HD: SATA, 128GB
- RAM: 2GB
- Adattatore di rete (necessario solo per l'ODV che opera in un ambiente di rete).
- Lettore CD/DVD, eventualmente accessibile tramite interfaccia USB (necessario solo per l'installazione dell'ODV).

7.3.2 Caratteristiche di sicurezza dell'ODV

7.3.2.1 Politica di sicurezza

La politica di sicurezza dell'ODV è espressa dall'insieme dei Requisiti Funzionali di Sicurezza implementati dallo stesso. Essa copre i seguenti aspetti:

- gli utenti dell'ODV devono essere ritenuti responsabili per le loro azioni rilevanti ai fini della sicurezza che a tal fine devono essere registrate;

- l'accesso ai dati ed alle funzioni dell'ODV deve essere concesso solo agli utenti autorizzati.

7.3.2.2 Ipotesi

Le ipotesi definite nel Traguardo di Sicurezza [TDS] ed alcuni aspetti delle minacce e delle politiche di sicurezza organizzative non sono coperte dall'ODV stesso. Tali aspetti implicano che specifici obiettivi di sicurezza debbano essere soddisfatti dall'ambiente operativo dell'ODV. In particolare, in tale ambito i seguenti aspetti derivati dal PP [PPGPOS] sono da considerare di rilievo:

- L'ODV risiede, per il suo utilizzo, su una piattaforma HW affidabile. Tale piattaforma è fuori dall'ambito della valutazione.

- Gli utenti autorizzati dell'ODV non possono essere considerati ostili o volutamente negligenti. Allo stesso tempo, un software malevolo potrebbe agire in qualità di utente e pertanto i requisiti che limitano i soggetti malevoli devono essere presi in considerazione.

- L'amministratore del sistema operativo non può essere considerato disattento, volutamente negligente o ostile, e si suppone amministri l'ODV nel rispetto della politica di sicurezza esistenti a livello operativo nell'ambiente d'uso.

7.3.2.3 Funzioni di sicurezza

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il cap. 8 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **Identificazione e autenticazione**: l'identificazione e l'autenticazione dell'utente all'ODV include le forme di accesso interattivo (ad es. utilizzando il protocollo SSH o il log in alla console locale) nonché il cambio di identità tramite il comando `su` o `sudo`. Tutti questi si basano su informazioni di autenticazione esplicite fornite in modo interattivo da un utente. In particolare, avviene quanto segue:

    - A tutti i singoli utenti viene assegnato un identificativo utente univoco all'interno del singolo sistema *host* che costituisce l'ODV. Questo identificativo utente viene utilizzato insieme agli attributi e ai ruoli assegnati all'utente come base per le decisioni relative al controllo degli accessi.

    - L'ODV autentica l'identità dichiarata dell'utente prima di consentire all'utente di eseguire ulteriori azioni.

    - L'ODV mantiene internamente un insieme di identificatori associati ai processi, che sono derivati dall'identificativo univoco dell'utente al momento del login dell'utente stesso. Alcuni di questi identificatori possono cambiare durante l'esecuzione del processo (ad esempio, utilizzando il comando `su`) secondo una politica attuata dall'ODV.

  L'ODV consente i seguenti metodi di autenticazione:

- *Autenticazione basata su password*: è fornita da “Pluggable Authentication Module” (PAM) e viene sempre utilizzata durante il processo di accesso nella console locale o nella console remota, e quando si diventa un altro utente (comando `su`). I meccanismi di controllo della qualità delle password sono offerti dall’ODV. Questi meccanismi sono applicati nel momento in cui la password viene cambiata.

- *Autenticazione basata su chiave pubblica*: viene utilizzata per avviare un accesso SSH senza fornire la password dell’utente come specificato dal protocollo SSH V2.

- **Audit**: l’ODV fornisce una capacità di audit che consente la generazione di record di audit per gli eventi critici di sicurezza. L'amministratore autorizzato può selezionare quali eventi vengono sottoposti a revisione e per quali utenti è attivo il controllo. L’ODV fornisce strumenti che aiutano l'amministratore autorizzato ad estrarre tipi specifici di eventi di audit, eventi di audit per utenti specifici, eventi di audit relativi a specifici oggetti del *file system*, o gli eventi di audit entro un determinato periodo di tempo sulla base dei dati complessivi di audit raccolti dall’ODV. I record di audit sono memorizzati in testo ASCII, non è necessaria alcuna conversione delle informazioni in forma leggibile dall'uomo.
  Il sistema di audit rileva quando la capacità della traccia di audit supera le soglie configurabili e l'amministratore autorizzato può definire le azioni da intraprendere quando la soglia viene superata.

- **Discretionary Access Control (DAC)**: il DAC limita l'accesso agli oggetti del *file system* in base alle liste di controllo di accesso (ACL) che includono le autorizzazioni UNIX standard per “user”, “group” e “others”. I meccanismi di controllo degli accessi proteggono anche gli oggetti IPC da accessi non autorizzati. Il meccanismo DAC viene utilizzato anche per garantire che gli utenti non affidabili non possano manomettere i meccanismi dell’ODV.

- **Riutilizzo degli oggetti**: gli oggetti del *file system* così come la memoria e gli oggetti IPC vengono cancellati prima che possano essere riutilizzati da un processo appartenente ad un utente diverso.

- **Gestione della sicurezza**: i servizi di gestione della sicurezza forniti dall’ODV sono utilizzabili dagli amministratori autorizzati per modificare la configurazione del TSF. Tutti gli utenti autorizzati sono in grado di modificare i propri dati di autenticazione.

- **Servizi crittografici**: l’ODV fornisce comunicazioni crittograficamente protette per consentire alle entità remote di accedere all’ODV stesso. Per l’utilizzo interattivo, viene fornita un’implementazione del protocollo SSH V2. L’ODV implementa il protocollo TLS v1.2 (o superiore) per fornire reti protette, autenticate, confidenziali e a prova di manomissione tra due computer. L’ODV fornisce primitive crittografiche che gli utenti e i servizi possono utilizzare per scopi non specificati. L’ODV è conforme allo standard LUKS per supportare la riservatezza della memorizzazione dei dati tramite spazio di archiviazione protetto crittograficamente: i dati cifrati possono essere decifrati solo dalla chiave di sessione dell'utente.

- **Protezione del TSF**: durante il funzionamento, il software del *kernel* e i dati sono protetti dai meccanismi di protezione della memoria hardware. I componenti di

gestione della memoria e dei processi del *kernel* assicurano che un processo utente non possa accedere allo *storage* del *kernel* o ad altri processi. Il software e i dati delle "non kernel TSF" sono protetti dal DAC e da meccanismi di isolamento dei processi. In generale, anche i file e le directory contenenti dati interni del TSF (ad esempio i file di configurazione) sono protetti dalla lettura da permessi DAC. L'ODV implementa e applica i seguenti meccanismi di autoprotezione che proteggono i meccanismi di sicurezza dell'ODV così come il software eseguito dall'ODV stesso:

- "Address Space Layout Randomization" per il codice dello spazio utente.
- "Stack buffer overflow protection" utilizzando gli "stack canaries".
- "Secure Boot" per garantire che la catena di avvio fino ad includere il *kernel* insieme all'immagine di avvio (initramfs) non sia manomessa.
- Gli aggiornamenti al sistema operativo vengono installati solo dopo che le loro firme sono state convalidate correttamente.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita al cliente insieme al prodotto.

La documentazione indicata contiene le informazioni richieste per l'inizializzazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.3 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] dichiara conformità *exact* ai seguenti Profili di Protezione e *Functional Package*:

- Protection Profile for General Purpose Operating Systems, Version 4.2.1 [PPGPOS]
- Functional Package for Secure Shell (SSH), Version 1.0 [FPSSH]
- Functional Package for Transport Layer Security (TLS), Version 1.1 [FPTLS]

7.6 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati o ricavati per estensione dai CC Parte 3 [CC3].

Tutti i Requisiti Funzionali di Sicurezza (SFR) sono stati derivati direttamente o ricavati per estensione dai CC Parte 2 [CC2].

Considerando che il TDS dichiara conformità *exact* al PP [PPGPOS] e ai FP [FPSSH] e [FPTLS], sono inclusi tutti e soli i SAR e gli SFR definiti in questo PP e nei relativi FP.

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, gli SFR e le funzioni di sicurezza che realizzano gli obiettivi stessi.

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM]. Inoltre, sono state eseguite tutte le attività di garanzia specifiche richieste dal PP [PPGPOS].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS Leonardo.

L'attività di valutazione è terminata in data 3 giugno 2022 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 20 giugno 2022. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B – Configurazione valutata. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS Leonardo e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "FIN.X RTOS SE V5" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia definito dai SAR inclusi nel PP [PPGPOS], in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia definito dai SAR inclusi nel PP [PPGPOS].

Classi e componenti di garanzia		**Verdetto**
Security Target evaluation	**Classe ASE**	Positivo
Conformance claims	ASE_CCL.1	Positivo
Extended components definition	ASE_ECD.1	Positivo
ST introduction	ASE_INT.1	Positivo
Security objectives	ASE_OBJ.2	Positivo
Derived security requirements	ASE_REQ.2	Positivo
Security problem definition	ASE_SPD.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Basic functional specification	ADV_FSP.1	Positivo
Guidance documents	**Classe AGD**	Positivo
Operational user guidance	AGD_OPE.1	Positivo
Preparative procedures	AGD_PRE.1	Positivo
Life cycle support	**Classe ALC**	Positivo
Labelling of the TOE	ALC_CMC.1	Positivo
TOE CM coverage	ALC_CMS.1	Positivo
Timely Security Updates	*ALC_TSU_EXT.1*	Positivo
Test	**Classe ATE**	Positivo
Independent testing - conformance	ATE_IND.1	Positivo
Vulnerability assessment	**Classe AVA**	Positivo

Classi e componenti di garanzia		Verdetto
Vulnerability survey	AVA_VAN.1	Positivo

Tabella 1 - Verdetti finali per i requisiti di garanzia

8.2 Attività di garanzia aggiuntive

Il PP [PPGPOS] e i FP [FPSSH] e [FPTLS] includono attività di garanzia aggiuntive che sono specifiche per il tipo di tecnologia dell'ODV e sono richieste per la conformità *exact* al PP e ai relativi FP.

I Valutatori hanno svolto le attività di garanzia richieste per tutti gli SFR definiti nel PP [PPGPOS] e nei FP [FPSSH] e [FPTLS] e inclusi nel Traguardo di Sicurezza [TDS]. L'obiettivo di queste sotto-attività è quello di determinare se sono soddisfatti tutti i requisiti delle attività di garanzia incluse nel PP e nei relativi FP.

I Valutatori hanno assegnato un verdetto "Positivo" a tutte le attività di garanzia incluse nel PP e nei relativi FP.

8.3 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "FIN.X RTOS SE V5" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel cap. 4.2 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le ipotesi descritte nel par. 3.3 del [TDS].

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata; in particolare, in Appendice A – Indicazioni per l'uso sicuro del prodotto sono incluse una serie di raccomandazioni relative alla consegna, all'inizializzazione, alla configurazione e all'utilizzo sicuro del prodotto, secondo le indicazioni contenute nella documentazione operativa fornita insieme all'ODV ([SUM]).

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

9.1 Consegna dell'ODV

Il Sistema Operativo FIN.X RTOS SE V5 viene consegnato su due supporti ottici di tipo CD-ROM o DVD-ROM:

1. un DVD-ROM etichettato CSCI_FINXSE_V5 "Installation Kit", che contiene tutti i file necessari per installare l'ODV nell'hardware di destinazione;

2. un CD/DVD-ROM etichettato CSCI_FINXSE_V5 "Integrity checks", che contiene tutti i file necessari per la verifica dell'integrità del Kit di installazione.

I due CD/DVD-ROM vengono consegnati separatamente, preferibilmente tramite corriere diverso. I contenuti del disco CSCI_FINXSE_V5 "Integrity checks" possono essere richiesti anche via Email al Fornitore MBDA.

Dopo aver ottenuto i due CD/DVD-ROM, l'utente amministratore incaricato dell'installazione dell'ODV deve prima verificare che la loro etichettatura sia coerente con le informazioni riportate nelle lettere di accompagnamento presenti all'interno dei pacchi consegnati e successivamente deve verificare l'integrità del Kit di installazione verificando il suo valore di *checksum* SHA-256 con quello fornito nel disco "Integrity checks".

Il Kit di installazione consente l'installazione dell'ODV nella sua configurazione certificata su una delle piattaforme hardware e di virtualizzazione supportate.

9.2 Installazione, inizializzazione e utilizzo sicuro dell'ODV

L'installazione, la configurazione e l'operatività dell'ODV devono essere eseguite secondo le istruzioni riportate nelle sezioni appropriate della documentazione di guida fornita con il prodotto al cliente.

In particolare, il documento "Software User Manual for the CSCI FIN.X RTOS SE V5" [SUM] contiene informazioni dettagliate per l'inizializzazione sicura dell'ODV, la preparazione del suo ambiente operativo e il funzionamento sicuro dell'ODV in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS].

10 Appendice B – Configurazione valutata

L'ODV, denominato "FIN.X RTOS SE V5" (P/N 16110074307.01, WI38500), è costituito dal *kernel* Linux x86_64-5.10.106 con la patch opzionale PREEMPT_RT e da un insieme di pacchetti software elencati nel par. 3.2 del documento "Software Version Document" [SVD].

La versione dell'ODV valutata è la 5.0 per architetture a 64-bit.

L'ambiente operativo su cui tale versione dell'ODV è stata valutata è costituito dalle piattaforme hardware elencate in Tabella 2 come specificato nel par. 1.5.3 del Traguardo di Sicurezza [TDS]:

Produttore	**Modello**	**CPU**
Concurrent Technologies	Board VP B1x	Intel® Core™ i7
Panasonic	TOUGHBOOK CF-54	Intel® Core™ i7
Larimart	LRT-314	Intel® Core™ i7
Themis	Rugged Enterprise Server XR5	Intel® Xeon®

Tabella 2 - Piattaforme hardware utilizzate per la valutazione dell'ODV

Il documento di guida "Software User Manual for the CSCI FIN.X RTOS SE V5" [SUM], che costituisce parte integrante dell'ODV, specifica un insieme di vincoli, come per esempio valori specifici di parametri contenuti nei file di configurazione, passi che devono essere eseguiti durante l'installazione e informazioni rivolte all'amministratore relativamente a come gestire in modo sicuro l'ODV.

11 Appendice C – Attività di test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia definito dai SAR inclusi nel PP [PPGPOS], tali attività non prevedono l'esecuzione di test funzionali da parte del Fornitore, ma soltanto test funzionali indipendenti e test di intrusione da parte dei Valutatori.

11.1 Configurazione per i test

Le attività di test sono state svolte presso la sede del Fornitore su un ambiente di test predisposto dal Fornitore stesso in accordo con i Valutatori.

L'ambiente di test è costituito da quattro istanze dell'ODV installate sulle piattaforme hardware elencate in Tabella 2, collegate tramite uno *switch* di rete che offre la possibilità di eseguire i test utilizzando il protocollo di rete SSH o tramite mouse. tastiera e monitor agganciati direttamente al sistema.

Tutti i test sono stati eseguiti dai Valutatori utilizzando due macchine di test (PC di tipo laptop) connesse alle istanze dell'ODV mediante lo *switch* di rete, tramite il protocollo SSH.

11.2 Test funzionali ed indipendenti svolti dai Valutatori

Il Traguardo di Sicurezza [TDS] dichiara conformità *exact* al PP [PPGPOS] e ai FP [FPSSH] e [FPTLS], che definiscono una serie casi di test mappati sugli SFR. Per soddisfare i requisiti di test del PP e dei relativi FP, i Valutatori hanno eseguito tutti i casi di test inclusi nella Test Suite del Fornitore e tutti quelli sviluppati indipendentemente dagli stessi Valutatori, soddisfacendo così anche i requisiti per ATE_IND.1.

Prima di iniziare l'attività di test, i Valutatori hanno verificato che l'ambiente di test fosse stato predisposto correttamente dal Fornitore e che le varie istanze dell'ODV fossero configurate correttamente.

Il materiale utilizzato dai Valutatori per l'esecuzione dei test è in parte contenuto in una Test Suite messa a disposizione dal Fornitore, non facente parte dell'ODV, ed in parte da una Test Suite e da procedure, costituite da comandi e linee di codice, sviluppate dai Valutatori. I Valutatori hanno eseguito la verifica del codice costituente la Test Suite del Fornitore, per assicurare la correttezza delle operazioni eseguite.

I Valutatori hanno eseguito tutti gli script facenti parte della Test Suite del Fornitore, che coprono gli SFR della classe funzionale "Cryptographic support" (FCS) inclusi nel PP [PPGPOS] e nell'FP [FPSSH], e tutti gli script inclusi nella Test Suite dei Valutatori, che realizzano un insieme di test relativi alle classi funzionali FMT e FPT presenti nel PP.

Per completare la copertura dei test richiesti dal PP e dai relativi FP, i Valutatori hanno definito una procedura per ciascun test indicato nella sezione "Assurance Activity" di ciascun SFR. Queste comprendono l'esecuzione di parti di codice *bash* (script) e/o l'esecuzione di sequenze di comandi da terminale.

Per l'esecuzione di alcuni dei test relativi al protocollo TLS i Valutatori hanno utilizzato gli strumenti software TLS-Attacker, Wireshark e TLS Test Tool (`tls-cc-tools`), uno strumento messo a disposizione dal NIAP che esegue per intero i passaggi necessari per il completamento dei test relativi al protocollo TLS.

In questo modo i Valutatori hanno eseguito tutti i test richiesti descritti nel PP [PPGPOS], nei FP [FPSSH] e [FPTLS] e nelle Technical Decision del NIAP applicabili elencate nel par. 2.2.1 del Traguardo di Sicurezza [TDS].

Tutti i test eseguiti dai Valutatori hanno fornito risultati coerenti con i risultati attesi.

11.3 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività, i Valutatori hanno operato sullo stesso ambiente di test già utilizzato per le attività di test funzionali, verificando che l'ODV e l'ambiente di test fossero correttamente configurati.

In una prima fase, i valutatori hanno effettuato una ricerca delle vulnerabilità note dei sistemi operativi Linux, con particolare riferimento a quelle del *kernel* utilizzato nell'ODV e della distribuzione Gentoo, tramite la consultazione di siti Web specializzati.

Successivamente, i Valutatori hanno verificato che i documenti di sviluppo e di guida operativa dell'ODV fossero adeguati nel fornire evidenza che non fossero presenti vulnerabilità introdotte nell'ODV durante lo sviluppo e nel modo di operare dell'ODV.

Infine, i valutatori hanno eseguito scansioni di vulnerabilità mediante uno strumento automatico (Tenable Nessus Professional) sulle varie piattaforme messe a disposizione per i test.

In seguito a tale analisi i Valutatori hanno determinato che sull'ODV non sono presenti vulnerabilità di rilievo, in quanto tutte le segnalazioni rilevate nei report di scansione risultano essere di livello informativo. I Valutatori hanno pertanto ritenuto non necessario approfondire l'analisi tramite attività di test di intrusione.

I Valutatori hanno quindi concluso che l'ODV, nel suo ambiente operativo, è in grado di resistere ad un attaccante che possiede un potenziale di attacco di livello Basic. Non sono state identificate vulnerabilità sfruttabili o residue.